ROBERT C. SCHUBERT (rschubert@sjk.law) (SBN 62684)
AMBER L. SCHUBERT (aschubert@sjk.law) (SBN 278696)
DANIEL L.M. PULGRAM (dpulgram@sjk.law) (SBN 354569)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Diane LaMarre, on behalf of herself and all others similarly situated,

Plaintiff,

v.

California Physicians' Service d/b/a Blue Shield of California,

Defendant.

No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Diane LaMarre ("Plaintiff"), on behalf of herself and on behalf of all others similarly situated alleges the following against Defendant California Physicians' Service d/b/a Blue Shield of California ("Defendant") upon personal knowledge as to her own acts, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. This is a class action against Defendant California Physicians' Service d/b/a Blue Shield of California ("Blue Shield" or "Defendant") brought on behalf of current and former Blue Shield subscribers whose personally identifying information ("PII") and personal health information ("PHI") was exposed to Google Analytics and Google Ads without their permission or consent. Blue Shield hired Google Analytics as a third-party vendor service to internally track usage of the Blue Shield website. Google Analytics, Google Ads, and other tracking tools are collectively referred to as "Tracking Technologies" or "Tracking Tools."

2. Although Blue Shield undoubtedly has a duty to protect patient PII and PHI, between at least April 2021 and January 2024, Blue Shield's Tracking Tools transmitted member information, including health information, to Google's advertising product, Google Ads. Although Blue Shield claims to have severed the connection between Google Analytics and Google Ads in January 2024, it paradoxically claims that it did not discover the connection between Google Analytics and Google Ads until February 11, 2025. Regardless of when Blue Shield became aware of or should have become aware of the breach, no subscriber was informed of the breach until, at earliest, April 9, 2025. Defendant had a duty to protect and secure sensitive subscriber data, including data provided to third parties, to sufficiently inform subscribers as soon as practicable of any data breach, and to abide by its own stated and agreed data security policies and procedures. Defendant's failures in these duties harmed Plaintiff and the class.

3. At all relevant times Defendant Blue Shield required healthcare subscribers, including Plaintiff, to provide highly sensitive PII and PHI to Defendant as a precondition for receiving healthcare services. At all relevant times Defendant set forth that its website was a safe and appropriate place to access, maintain, and update subscriber PII and PHI.

4. Defendant collects, stores, and maintains significant PII and PHI on its current and former subscribers through its website.

5. Defendant shared significant PII and PHI from at least hundreds of thousands of current and former subscribers with Google Ads, who in turn may have shared it with their own partners, affiliates, or data purchasers.

6. The information breached is highly sensitive and includes at least subscriber full name, gender, full address, insurance plan name, insurance plan type, insurance plan group number, Blue Shield identifiers for members' online accounts, medical claim service data and service provider, patient financial information, find a doctor search criteria, and results including location, plan name and type, healthcare provider name, and type.

7. Although Blue Shield claims this information was only shared with Google Analytics, which shared the information with Google Ads, on information and belief, Google Ads uses its information not only to sell targeted ads, but it also may make that information available to additional third-party purchasers.

8. But for Defendant's creation and implementation of Google Analytics into its website, subscriber data would not have been breached. Blue Shield was responsible for securing its own website, but for years operated a website that surreptitiously transmitted private health data to an unknown third party, directly in contravention of the law and its duties to subscribers.

9. Because Blue Shield was responsible for configuring its own website to be secure, it should have immediately known that subscriber personal data was being scraped by Google as soon as the connection was set up, rather than allowing it to persist for years. At *minimum*, Blue Shield should have known about the data breach in January 2024 when it purports to have disabled the secret data sharing with Google. Nevertheless, Blue Shield maintains it did not discover a years-long sensitive data breach until February 2025.

10. Although Defendant described the events as a data breach, this is a highly unusual privacy violation as Defendant *intentionally and deliberately* used Tracking Tools on its website, which resulted in the disclosure of information to Google. It was greed, carelessness, and indifference which led to the unauthorized disclosure of protected subscriber information.

11. Defendant is a major healthcare insurance company with thousands of employees and millions of members. Its revenue is easily in the billions of dollars. Defendant has and had the resources to adequately secure subscriber data, maintain the security of its website, and to vet third-party service providers to ensure those service providers had adequate security and that private information was not inadvertently shared with them.

12. Defendant is well-aware that both it and the third-party services it utilizes are at high risk of attempted cyberattack due to the high value of the sensitive data. Indeed, Defendant Blue Shield has had its subscriber data exposed in other data breaches. For example, on November 17, 2023, Blue Shield announced that a "cybersecurity attack on vendor's files may have impacted Blue Shield of California Member Data." This data breach, which Defendant became aware of at least as early as September 1, 2023,[1] involved another third-party service provider it utilized—MOVEit. Likewise, in yet another data breach involving yet another third-party service provider, sensitive Blue Shield subscriber information was breached by Young Consulting, a contractor hired by Blue Shield. In that data breach, Blue Shield became aware of the breach in April 2024, but did not begin to inform subscribers until late August 2024.

13. Defendant has repeatedly exposed subscriber information through third-party Vendors. Defendant was fully aware of the risk that other breaches might occur involving third parties it provided information to. This Google Analytics data breach is yet another instance in Blue Shield's long and discreditable history of insufficiently securing customer data especially when third-party vendors or service providers are involved. Blue Shield can do better, but has not.

14. Defendant is also a participant in the California Statewide Data Sharing Agreement.[2] This agreement sets forth numerous security and data sharing standards including requirements for responses to data breaches. Among other factors, Defendant participated in the statewide agreement which, among other things, states as follows:

[1] https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (Last Accessed September 15, 2024)

[2] https://www.blueshieldca.com/content/dam/bsca/en/member/docs/Blue-Shield-of-California-2023-Mission-Report.pdf (Last Accessed September 16, 2024) at 22.

> Breaches can be very serious events with potential for serious impact on Participants and the individuals whose Health and Social Services Information is breached. This policy requires each Participant to identify, notify, investigate and mitigate any Breach and, when detection of a Breach has occurred, to notify CDII and any Participants impacted by the Breach in accordance with the procedures herein. This policy shall be effective as of January 31, 2024.[3]

Defendant expressly acknowledged that data Breaches, such as the breach at issue here, can be very serious events with potential for serious impact on Participants and their individual subscribers whose information was breached. Defendant had full knowledge of the value of this information and the risk of a breach. Despite this, Defendant deliberately activated and used the Tracking Tools.

15. Despite Defendant's awareness of both the value and sensitivity of the data it safeguarded and serious risk that insufficient security practices by vendors presents, Defendant did not take sufficient steps to ensure that its website was secure and that sensitive data was not being scraped from every customer who used it. Defendant knew or should have known about the risk to the data they stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

16. Despite knowing the risks, Defendant knowingly disclosed subscribers' PHI and PII to Google. Google Analytics cannot collect data from a website *unless the website is configured to permit the data collection.* Intentionally or otherwise, disclosing the PHI and PII to Google was and is a massive security failure.

17. The failure to implement adequate data security measures is extraordinary negligence. This was not one day or one week of the website having the wrong settings; Blue Shield sent sensitive subscriber data to Google for *years* without the subscribers' knowledge or consent. Blue Shield's inability to secure its own website is alarming.

18. Moreover, Defendant's failure to notify subscribers that they had been impacted by this data breach for at least two months after Defendant became aware of the breach harmed Plaintiff and made it more difficult for Plaintiff to take swift action to respond to the breach.

[3] https://www.cdii.ca.gov/wp-content/uploads/2023/12/CalHHS_Breach-Notification-PP_Final_v1.0.1_12.11.23.pdf

Defendant's failure to timely notify subscribers also plainly violated their obligations under the Statewide Data Sharing Agreement that it is a participant in.

19. Plaintiff and Class members have been harmed because they are at immediate risk of having their personal information used against them. Indeed, they have been at risk well before Defendant even notified Plaintiff of the breach. Plaintiff does not know what Google Ads has done with her data and if it has been sold, transferred, replicated, or irrevocably disseminated exposed. She suffered harm in the loss of the value of her data which cannot be easily recovered, if ever.

20. Blue Shield has not identified how, if at all, it is attempting to claw back the data it gave (or perhaps even sold) to Google, or whether Google may have sold the data to additional third parties. Blue Shield has also not offered any identity theft monitoring services as a result of the breach. This creates uncertainty about the extent to which subscribers have been harmed and the need to engage in various services and efforts in the wake of the data breach, including but not limited to examining whether their PII or PHI has been sold on the dark web, taking measures to protect against identity theft crimes, expenses, and/or time spent on credit monitoring and identity theft insurance, time spent examining bank statements, time spent initiating fraud alerts, and other consequential harms.

21. Blue Shield cannot abrogate its responsibility to ensure that customer data is protected merely by contracting with third parties for analytical services, especially on Blue Shield's own website, which it invites subscribers to utilize!

22. Plaintiff, individually and on behalf of a nationwide class, alleges claims of (1) Negligence; (2) Breach of Implied Contract; (3) Unjust Enrichment; (4) violation of California's Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq.*); (5) violation of California's Unfair Competition Law (Cal. Civ. Code §§ 17200, *et seq.*); (6) violation of California's Confidentiality of Medical Information Act (CMIA) (Cal. Civ. Code § 56.10); (7) violation of California Penal Code § 631, *et seq.* (Invasion of Privacy Act); (8) violation of California Penal Code § 638.51(a); (9) Violation of California Constitution, Article 1 § 1; (10) Violation of the Electronic Privacy Act, 18 U.S.C. § 2510, et seq; (11) Intrusion upon seclusion; (12) Publication of Private Facts; and (13) Breach of Confidence. Plaintiff also seeks declaratory and injunctive relief. Plaintiff asks the

Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

23. Plaintiff Diane LaMarre is a resident of Fremont, California. She brings this case on behalf of herself and all others similarly situated.

24. Plaintiff LaMarre was a Blue Shield subscriber, and her personal information was exposed as a result of the Google Analytics Data Breach.

Defendant

25. Defendant California Physicians' Service d/b/a Blue Shield of California is a major California health care insurer. As of December 2023, it purported to have 4.8 million members, 7,119 employees, and over 25 billion dollars in revenue.[4] It operates offices throughout California and its headquarters is at 601 12th Street, Oakland, California 94607.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The class contains more than 100 members, and many of these members have citizenship diverse from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the case in controversy.

27. The exercise of personal jurisdiction over Defendant is appropriate. Blue Shield of California is a California corporation and its principal place of business is in this District.

28. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District. Specifically, Blue Shield's principal place of business is in this

[4] https://www.blueshieldca.com/content/dam/bsca/en/member/docs/Blue-Shield-of-California-2023-Mission-Report.pdf (Last Accessed September 16, 2024)

district, it is headquartered in this district, it is a California corporation, and Defendant's methodology for assessing website security and privacy protections, vendor security systems, representations, decision-making, and security practices emanated from this District.

29. Divisional Assignment: This action arises in Alameda County, in that a substantial part of the events which give rise to the claims asserted herein occurred in Alameda County, where Defendant is headquartered and located. Pursuant to L.R. 3-2(d), all civil actions that arise in Alameda County and San Francisco County shall be assigned to the San Francisco or Oakland Division.

FACTUAL ALLEGATIONS

I. Background

30. Blue Shield is a major California healthcare insurer. It has 4.8 million subscribers (members), 7,119 employees, and in excess of $25 billion in annual revenue as of December 2023.[5]

31. Google (parent company, Alphabet) is a massive international technology conglomerate. At least between April 2021 and January 2024, Blue Shield used Google Analytics as a third-party vendor service to track website usage for members who used Blue Shield sites. This information was provided to at minimum Google Ads.

32. Plaintiff and class members are former or current insured individuals who obtained insurance from Blue Shield of California and had PHI and/or PII exposed as a result of the Google Analytics Data Breach.

33. In order to receive treatment, Plaintiff and Class members were required to provide all or part of the following non-exclusive list of sensitive PHI and PII during the regular course of business:

- Full name and mailing or personal address,
- State and/or Federal Identification,
- Social Security Number,

[5] https://www.blueshieldca.com/content/dam/bsca/en/member/docs/Blue-Shield-of-California-2023-Mission-Report.pdf

- Health insurance information including but not limited to carrier, policy number, and healthcare card,
- Date of birth,
- Medical information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health information, information related to STDs and treatment, medication information, and medical record number,
- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient,
- Residence and travel history,
- Billing and claims information including but not limited to information related to credit and debit card numbers, bank account statements and account numbers, and insurance payment details.
- Medicare/Medicaid information.
- Information on prescriptions taken including history of taking certain prescriptions.
- Diagnostic results and treatment information.
- Information on family members including but not limited to emergency contact information and next of kin.
- Personal email addresses and phone numbers.
- Workers' comp and employment related information

34. The above information is extremely sensitive personal identifying information and personal health information (PII and PHI). This information is extremely valuable to criminals because it can be used to commit serious identity theft and medical identity theft crimes.

35. Some or all of this extremely sensitive information is required to be entered or is otherwise displayed on Blue Shield's website. Although Blue Shield claims that social security numbers, driver's license numbers, and banking or credit card information was not breached, the remaining information that was surreptitiously leaked to Google for years is still incredibly private and valuable. At minimum the information sent to Google includes: "Insurance plan name, type

and group number; city; zip code; gender; family size; Blue Shield assigned identifiers for members' online accounts; medical claim service date and service provider, patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type)."[6]

II. The Breach

36. At least as early as April 2021, Blue Shield installed Google Analytics on Blue Shield's website in a configuration that allowed private member data to be shared with Google. This constituted a massive data breach.

37. Blue Shield claims that it "severed" the connection between Google Analytics and Google Ads in January 2024. Despite claiming to have severed the connection in January 2024, Blue Shield confusingly claims it didn't discover the connection until February 11, 2025.

38. It is unclear why this breach was allowed to persist for years, or why Blue Shield somehow remained ignorant of the data breach despite claiming to take action to sever it in January 2024.

39. The data breach impacted at least hundreds of thousands of subscribers and, as described above, included highly sensitive PII and PHI including but not limited to: "Insurance plan name, type and group number; city; zip code; gender; family size; Blue Shield assigned identifiers for members' online accounts; medical claim service date and service provider, patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type)."

40. It took Blue Shield nearly two months after the purported February 2025 discovery of the breach to begin to notify subscribers. Blue Shield does not explain the delay. It should have notified Subscribers immediately of the breach, not waited nearly 2 months.

41. It is unclear whether Blue Shield is attempting to retrieve and delete the sensitive data gathered by Google or if that is even possible given Google may have shared the sensitive PHI and PII with its own partners, affiliates, and other data purchasers. It is also unclear how Blue

[6] https://news.blueshieldca.com/notice-of-data-breach (Last Accessed April 11, 2025)

Shield discovered the breach, including whether or not they discovered it themselves or had to be informed of the breach by Google.

42. As of April 11, 2024, Blue Shield has not disclosed the precise cause of the data breach, the efforts, if any, Blue Shield has taken to mitigate the harm to subscribers and limit the spread of the leaked data or offered any remedy for impacted subscribers. Google Ads typically pays for analytics data, and it is unclear if Blue Shield was paid or received a lower fee from Google Analytics in exchange for sharing subscriber information without prior authorization or consent.

III. Defendant Failed to Comply with Cybersecurity Standards

43. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding its subscribers' PII and PHI, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII and PHI for a significant number of customers, a significant number of customers would be harmed by a breach of its systems and its website in particular. Defendant further knew due to the nature of its business practices as a major health insurance provider that the data it was entrusted with was highly valuable and contained private and sensitive information including medical information.

44. Defendant makes numerous data representations on its website concerning the care they take to protect customer data, their use of the data, and privacy policy. Defendant also represents in its 2023 year-end "Mission Report" that it would "carefully [protect] members' data" and that it was a participant in the California Statewide Data Sharing Agreement ("DSA").[7]

45. The DSA contains numerous standards and requirements for Participants, such as Defendant, concerning the use, security procedures, and sharing of individual personal and health information. Blue Shield made public statements concerning their participation in the DSA and indeed is listed as a signatory/participant in the associated California Government Directory.[8]

[7] https://www.blueshieldca.com/content/dam/bsca/en/member/docs/Blue-Shield-of-California-2023-Mission-Report.pdf

[8] *See* https://www.cdii.ca.gov/wp-content/uploads/2023/06/DxF_DSA_SignatoryList.xlsx

46. By signing on to the DSA as a Participant and advertising its participation in the program, Defendant represented that it would use and employ data sharing and security practices and procedures consistent with the requirements of the DSA. Defendant therefore had a duty to abide by those same standards.

47. Defendant failed to abide by the DSA standards, and this failure directly harmed Plaintiff and the class. These failures include but are not limited to as follows:

- **Representations and Warranties – *Third Party Technology***

  Pursuant to the DSA Defendant was required to:

  > "[H]ave agreements in place that require Third-Party Technology vendors (i) to provide reliable, stable, and secure services to the Participant [Blue Shield], and (ii) to adhere to the same or similar privacy and security standards applicable to the Participant pursuant to this Agreement"[9]

Google Analytics and Google Ads in particular do not and did not provide sufficiently "secure services," nor did it adhere to the "privacy and security standards applicable to the Participant." Thus, Defendant does not appear to have complied with the requirement for representations and warranties applicable to Third Party Technology providers, such as Google Analytics.

- **Minimum Necessary Information Disclosure**

Defendant also agreed that "Any use or disclosure of PHI or PII pursuant to this Agreement will be limited to the minimum PHI or PII necessary to achieve the purpose for which the information is shared"[10] There appear to be no legitimate purpose whatsoever for the disclosure of sensitive PHI and PII to Google Ads, let alone the potential downstream effects of such a disclosure. This plainly violates Defendant's requirement to only provide "Minimum Necessary Disclosure." The information leaked, including PHI and PII, cannot be a *necessary* disclosure to Goole Ads when the information is being secretly shared without the knowledge of subscribers and is not being used in connection with the provision of *any* medical services.

- **Data Breach Notification Requirements:**

[9] https://www.cdii.ca.gov/wp-content/uploads/2023/01/1.-CalHHS_DSA_Final_v1_7.1.22-11.8.22.pdf
[10] https://www.cdii.ca.gov/wp-content/uploads/2023/01/1.-CalHHS_DSA_Final_v1_7.1.22-11.8.22.pdf

The DSA sets forth several Data Breach Notification requirements, many of which Defendant has violated as laid out by subsection on "Breach Notification" which became effective on January 31, 2024.[11] Specifically, Defendant failed to do the following:

- "As soon as reasonably practicable after discovering a breach has occurred … a participant shall notify CDII and all Participants impacted by the breach."
  - At best, Defendant waited at least two months after they were notified of the breach to send any kind of notification to impacted members.
- "As soon as reasonably practicable after discovering a Breach has occurred… a Participant shall provide a written report of the Breach to all Participants impacted by the Breach. The Participant shall supplement the information contained in the written report as it becomes available and shall cooperate with other impacted Participants… Such written report should include, to the extent available, the following information:

  i. One or two sentence description of the breach

  ii. Description of the roles of the people involved in the Breach (e.g., employees, service providers, unauthorized persons);

  iii. The type of Health and Social Services Information Breached;

  iv. Participants likely impacted by the Breach;

  v. Number of individuals or records impacted/estimated to be impacted by the breach;

  vi. Actions taken by the participant to mitigate the Breach;

  vii. Current status of the Breach (under investigation or resolved); and

  viii. Corrective action taken and steps planned to prevent a similar Breach"[12]

48. Defendant has not described the roles of any of the persons involved in this breach or specified the number of individuals or records impacted or estimated to be impacted Defendant has not described any actions that it is taking to mitigate the data breach. Indeed, the *entirety* of

[11] https://www.cdii.ca.gov/wp-content/uploads/2023/12/CalHHS_Breach-Notification-PP_Final_v1.0.1_12.11.23.pdf

[12] https://www.cdii.ca.gov/wp-content/uploads/2023/12/CalHHS_Breach-Notification-PP_Final_v1.0.1_12.11.23.pdf (Last Accessed September 16, 2024)

the section on Defendant's Data Breach Notice describing "What we [Blue Shield] are doing" reads as follows:

> **What we are doing:**
>
> We understand receiving a notice such as this can create concern, and we regret that member personal information may have been shared without authorization. Blue Shield takes the security of member information very seriously, and we are committed to maintaining their privacy.[13]

49. Blue Shield does not describe *any* efforts to retrieve or ensure the deletion of illegally shared information with Google Ads, any efforts to stop or stem downstream effects from data which may have been sold to additional third parties, or even discuss any internal changes to security policy and practices as a result of the breach. Although Blue Shield claims to take the "security of member information very seriously." The string of recent data breaches involving Blue Shield suggests otherwise. Blue Shield did not outline any corrective action taken or steps planned to prevent a similar breach in the future or efforts to stop Google from using information already shared.

50. A reasonable data breach letter would have provided at minimum the information listed above. Blue Shield's failure to provide the reasonably required information to participants in its healthcare plans has hampered the ability for Plaintiff and the class to effectively respond to the breach and has created confusion, stress, and has otherwise harmed the class.

51. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

52. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should

[13] https://news.blueshieldca.com/notice-of-data-breach (Last Accessed 4/11/2025)

implement to protect PII.[14] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

53. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

54. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

55. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

56. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

57. Defendant knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[15]

58. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

[14] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed March 21, 2024)

[15] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. (last accessed March 21, 2024)

59. This breach is particularly egregious because Defendant *specifically* configured its website in such a way that private PHI and PII was shared with Google Ads for years. In the absence of Defendant's abject negligence with ensuring the security of the data entered onto its website, this breach would not have occurred. Defendant was not employing reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' PII and PHI. If Defendant had implemented adequate security and monitoring measures, a misconfiguration should not have occurred or should have been corrected quickly, not allowed to persist for years.

60. Once Defendant became aware of the breach, it could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including taking *any* steps whatsoever to attempt to mitigate the harm caused by the breach.

61. Although Blue Shield claims "no bad actor was involved," there is no reason to believe the harvested data remains secure. Blue Shield has not disclosed whether Google Analytics, Google Ads, or other individuals, organizations, or services who could have purchased or used the data from Google Ads in a way that creates significant downstream effects or potentially exposes the data to criminal elements. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

62. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend

hundreds of hours fixing the damage caused by identity thieves.[16] Plaintiff and Class members generally have spent considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[17]

63. The information compromised in the Data Breach—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Defendant subscribers at additional risk for potential medical fraud and medical identity theft.

64. Data breaches and disclosures involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[18] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[19] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

65. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a. Maintaining a secure firewall

b. Monitoring for suspicious or unusual traffic on the website

---

[16] https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf. (last accessed September 6, 2024)

[17] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed September 6, 2024)

[18] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 22, 2023).

[19] *Id*

c. Looking for trends in user activity including for unknown or suspicious users

d. Looking at server requests for PII

e. Looking for server requests from VPNs and Tor exit notes

f. Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

g. Structuring a system including design and control to limit user access as necessary, including a user's access to the account data and PII of other users.

66. Defendant had a duty to ensure that not only did it comply with all these reasonable security measures, but to also ensure that its vendors met the same standards. Defendant should never have installed the Tracking Tools, especially if it was not completely sure about the security of the service. Defendant had an obligation to provide superior security in light of the sensitivity of the information they administered and to ensure that they did not inappropriately abrogate that obligation. Defendant *deliberately* configuring its website to use the Tracking Tools was more than just a data breach, Defendant intentionally opened the door to allowing unauthorized access to extremely sensitive information by Google Ads, which is among other things a data usage and sale organization. Defendant failed in its duty to protect and use reasonable security measures to protect subscriber data by its own deliberate actions.

IV. Plaintiff's and Class Members' Experiences

67. To use Defendant's Service, Plaintiff provided sensitive PII and PHI including her full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and other sensitive medical data. Although Defendant has not clarified all the information that was breached, it includes at least: Insurance plan name, type and group number; city; zip code; gender; family size; Blue Shield assigned identifiers for members' online accounts; medical claim service date and service provider, patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type).

68. Plaintiff has taken reasonable steps to maintain the confidentiality of her PII and PHI. When Defendant accepted Plaintiff and class members as subscribers, it assumed a duty to

store the data they provided in a way which was secure, and it did so with the implicit understanding it would be required to use its experience and sophistication to keep this information secure and confidential.

69. As a result of the data breach, Plaintiff was forced to take measures to mitigate the harm, including spending time monitoring credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

70. As a result of the Data Breach, Plaintiff suffered actual injuries including: (a) damages to and diminution in the value of Plaintiff's PII and PHI—property that Plaintiff entrusted to Defendant as a condition of receiving its services; (b) loss and invasion of Plaintiff's privacy; and (c) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of herself and a Nationwide Class defined as follows:

> **All current and former Blue Shield of California subscribers in the United States whose PII and/or PHI was disclosed to Google or other third parties by the Data Breach announced by Blue Shield in April 2025.**

72. Within the Nationwide class there is one California Subclass defined as follows:

> **All current and former Blue Shield of California subscribers who are California Residents and whose PII and/or PHI was disclosed to Google other third parties by the Data Breach announced by Blue Shield in April 2025.**

73. Excluded from the Nationwide Class and Subclass are governmental entities, Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

74. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

75. **Numerosity.** The Nationwide Class is so numerous that the individual joinder of all members is impracticable. While the exact number of Nationwide Class Members is currently unknown and can only be ascertained through appropriate discovery, Plaintiff, on information and belief, alleges that the Nationwide Class includes at least hundreds of thousands of members.

76. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that Google Analytics was not secure and that its use jeopardized private customer data;

b. Whether Defendant was paid by Google Analytics, Google Ads, or any other entity in exchange for the disclosure of subscriber PII and PHI.

c. Whether Defendant failed to take adequate and reasonable measures to ensure its website and data systems were protected;

d. Whether Defendant failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;

e. Whether Defendant unreasonably delayed in notifying subscribers of the harm they suffered once the suspicious activity was detected;

f. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

g. Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII and PHI;

h. Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

i. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

77. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

78. **Adequacy of Representation.** Plaintiff is an adequate class representative because she is a Nationwide Class Member, a California Subclass Member, and her interests do not conflict with the Class interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and her counsel intend to prosecute this action vigorously for the Class' benefit and will fairly and adequately protect their interests.

79. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class member's claim is impracticable. Even if each Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

80. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or

refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiff and the Class

81. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

82. Plaintiff was required to provide PII and PHI as a precondition for receiving insurance services from Defendant. Plaintiff and Class Members entrusted their PII and PHI to Defendant with the understanding that it would safeguard their PII and PHI.

83. Defendant likewise made numerous representations about its data security practices including that it was a participant in the California Statewide Data Sharing Agreement ("DSA"), which provides certain data sharing requirements and standards. This included representations it would minimize unnecessary data sharing with third party vendors.

84. Defendant did not take reasonable and appropriate safeguards to protect Plaintiff and Class Members' PII and PHI from disclosure to unauthorized third parties.

85. Defendant violated its obligations under the DSA as outlined on Defendant's website. Defendant also did not vet or otherwise sufficiently verify that its third-party vendor service, Google Analytics, used and maintained adequate security practices or would not share its data with Google Ads or other entities.

86. Defendant failed to create a secure website and indeed configured its website in such a way that private customer data would routinely be scraped by Google Analytics and sent to Google Ads.

87. In the absence of action deliberately configuring the website to function this way, information would not be sent to Google. Defendant's actions were willful and, at minimum, negligent with respect to their admitted duty to secure and limit the sharing of Private Information.

88. Defendant had full knowledge of the sensitivity of the PII and PHI that it stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

89. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's and Defendant's contractors' information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify patients of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed. It was not a reasonable security procedure and practice for Defendant to configure its website in such a way that subscriber PII and PHI could be scraped for years by third-party advertising and data services.

90. Defendant's duty of care arose from, among other things,

a. Defendant's exclusive ability (and Class Members' inability) to ensure that its systems, website, and vendor services were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

c. Defendant's participation in the DSA, including its assent to follow numerous data security measures outlined in the agreement.

d. Defendant's common law duties to adopt reasonable data security measures to protect customer PII and PHI and to act as a reasonable and prudent person under the same or similar circumstances would act.

91. Defendant's violation of the FTC Act constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were

designed to protect a group to which Plaintiff belong and to prevent the types of harm that resulted from the Data Breach.

92. Likewise, the DSA expressly discusses the risk of data breaches in the health industry and the impact that exposure of this information may have on individual subscribers. One of the plain purposes of the DSA is to ensure insurers, like Defendant, follow and enact sufficient data security practices and procedures.

93. Defendant processes sensitive information for millions of subscribers and has annual revenue in the tens of billions of dollars. Defendant had the financial and personnel resources necessary to prevent the Data Breach. Defendant nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members.

94. Plaintiff and Class Members were the foreseeable victims of Defendant's inadequate data security. Defendant knew that a breach of its systems or its contractors' systems could and would cause harm to Plaintiff and Class Members.

95. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included its failure to adequately mitigate harm through negligently failing to inform patients and victims of the breach of the specific information breached for (as of time of writing) more than four months after the purported first discovery of the breach.

96. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI and the importance of limiting disclosure of that PII and PHI, especially given the frequent data breaches Blue Shield has suffered.

97. Defendant, through its actions and inactions, breached its duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in its possession and control. Defendant breached its duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices, configuring its website to ensure data would only be shared with authorized third parties.

98. Defendant inadequately safeguarded consumers' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach. Defendant also breached its duties as outlined by the DSA.

99. But for Defendant's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

100. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach/unauthorized disclosure, and the harms suffered by Plaintiff and Class Members.

101. As a result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer the damages alleged herein.

102. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

103. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 2
Breach of Implied Contract
On behalf of Plaintiff and the Class

104. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

105. Plaintiff and Class Members were required to provide sensitive personal and health information to Defendant as a precondition for receiving health insurance services. As part of this exchange, there was an implied contract with Defendant when Defendant accepted custody of their PII and PHI.

106. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

107. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with the legal requirements, industry standards, and Defendant's own representations. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

108. Plaintiff and Class Members would not have provided and entrusted their PII and PHI to Defendant or would have paid less for Defendant's products or services in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiff and Class Members was critical to realize the intent of the parties.

109. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

110. Defendant breached their implied contracts with Plaintiff and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) configured their website in a way that secretly disclosed that information to unauthorized third-party advertising services for years and; (3) failed to notify Plaintiff and Class Members of the specific data breached in a reasonably timely manner.

111. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time

spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

112. As a direct and proximate result of the breach/unauthorized disclosure, Plaintiff and class members are entitled to relief as set forth herein.

113. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 3
Unjust Enrichment
On behalf of Plaintiff and the Class

114. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

115. This count is brought in the alternative to Plaintiff's breach of third-party beneficiary contract count.

116. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant for healthcare insurance services and provided Defendant with their PII and PHI. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members.

117. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form monetary payment and disclosure of PHI and PII as a necessary part of their receiving healthcare services. Defendant appreciated and accepted that benefit.

118. Upon information and belief, Defendant funds its data security measures and website from its general revenue, including payments made by Plaintiff and Class Members. As

such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security including the protection of the data from inadvertent disclosure to third parties. Defendant's website and it's security and privacy measures are entirely under the sole control of Defendant.

119. Defendant, however, failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided. Indeed, Defendant may have deliberately sold sensitive PII and PHI to third party advertising services or otherwise benefitted from the exchange. In any event, Plaintiff's private PHI and PII was provided to unauthorized third parties for years without Plaintiff's knowledge or consent.

120. Defendant would not be able to carry out an essential function of its regular business without the money and Private Information provided Plaintiff and Class Members. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

121. Defendant acquired the Private Information through inequitable means in that it failed to disclose the third party entities, like Google, that it provided the information to and the inadequate security practices previously alleged.

122. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, including by not reasonably ensuring the security of third-party vendors Defendant utilized, they would not have provided their Private Information to Defendant or would have paid less for Defendant's services.

123. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and cheaper contractors and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate

result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

124. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

125. Plaintiff and Class Members have no adequate remedy at law.

126. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. It is unknown where the data went after it was provided to Google Ads, but there is no reason to believe the disclosure to Google Ads was limited to Google Ads only or that the data did not pass through the stream of commerce to additional third parties. Plaintiff's injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

127. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members were underpaid by Defendant.

128. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 4
California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*
On behalf of Plaintiff and the California Subclass

129. Plaintiff, individually and on behalf of the Subclass, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

130. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

131. Defendant is a business that owns, maintains, or licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

132. Defendant violated Cal. Civ. Code § 1798.81.5 by failing to implement reasonable measures to protect California Subclass members' PII and PHI.

133. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII and PHI has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

134. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

135. Plaintiff and California Subclass Members' PII and PHI includes personal information identified in Cal. Civ. Code § 1798.82(h) such as their names, Social Security

numbers, address and date of birth, and health insurance information, and is thereby covered by Cal. Civ. Code § 1798.82.

136. Plaintiff and the California Subclass Members are "customers" within the meaning of Cal. Civ. Code § 1798.80(c), as their personal information was provided to Defendant for the purpose of utilizing Defendant's healthcare insurance services.

137. The Data Breach constituted a breach of Defendant's security systems, networks, and servers.

138. Because Defendant reasonably believed that Plaintiff and California Subclass Members' PII and PHI was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

139. Defendant unreasonably delayed informing Plaintiff and the California Subclass Members about the breach of security of their PII and PHI after learning of the breach in February 2025. Specifically, Defendant knew about the data breach at least as early as February 2025, but filed to notify Plaintiff or Subclass Members until April 2025.

140. Upon information and belief, no law enforcement agency instructed Defendant that notification to California Subclass Members would impede an investigation.

141. Thus, by failing to disclose the Data Breach in a timely and accurate manner, the Defendant also violated Cal. Civ. Code § 1798.82.

142. Pursuant to Cal. Civ. Code § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

143. As a direct and proximate result of Defendant's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members were (and continue to be) injured and suffered (and will continue to suffer) damages, as described above.

144. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages, any applicable statutory damages, and equitable and injunctive relief.

145. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 5
California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*
On behalf of Plaintiff and the California Subclass

146. Plaintiff, individually and on behalf of the Subclass, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

147. Plaintiff pleads this claim for equitable relief, including restitution and injunctive relief, in the alternative to her claims for damages.

148. Defendant violated California's Unfair Competition Law (the "UCL"), Cal. Bus. & Prof. Code §§ 17200 *et seq.*, by engaging in unlawful, unfair, or fraudulent business acts and practices that constitute acts of "unfair competition" as defined in the UCL with respect to their conduct and actions with towards Plaintiff and the California Subclass.

149. Defendant's actions as alleged herein in this Class Action Complaint constitute an "unlawful" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq.* because Defendant's actions: (a) violated the California Consumer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, (b) constituted negligence; and (c) violated federal law and regulations, including the FTC Act and HIPAA.

150. Defendant's actions as alleged in this Class Action Complaint also constitute an "unfair" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq.*, because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious. The harm caused by Defendant's wrongful conduct outweighs any utility of such conduct and has caused—and will continue to cause—substantial injury to the California Subclass, including Plaintiff LaMarre. There were ample reasonably available alternatives that would have furthered Defendant's legitimate business practices, including basic understanding of website

design, security, analytics, and data scraping. Additionally, Defendant's conduct was "unfair" because it violated the legislatively declared policies reflected by California's strong data-breach and online-privacy laws, including the California Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and the California's Confidentiality of Medical Information Act (CMIA)(Cal. Civ. Code § 56.10).

151. As a result of Defendant's unlawful and unfair conduct, Plaintiff and the California Subclass were damaged and injured by the significant costs of protecting themselves from identity theft and face ongoing and impending damages related to loss of control over their PII and PHI.

152. Defendant's wrongful practices constitute a continuing course of unfair competition because, on information and belief, Defendant has failed to remedy the lax security practices or even fully notify all affected California persons. Plaintiff and the California Subclass seek equitable relief pursuant to Cal. Bus. & Prof. Code § 17203 to end Defendant's wrongful practices and require Defendant to maintain adequate and reasonable security measures to protect the PII and PHI of Plaintiff and the California Subclass.

153. Plaintiff and California Subclass Members lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, ongoing identity theft and fraud, as well as long term incalculable risk associated with medical fraud.

154. Further, if an injunction is not issued, Plaintiff and California Subclass Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Defendant has still not provided adequate information on the cause and scope of the Data Breach or what efforts, if any, it is taking to attempt to claw back patient data from Google Ads or any third parties who may have utilized Google Ads or whom Google Ads or Analytics may have sold the data to. Plaintiff and California Subclass Members lack an adequate remedy at law that will reasonably protect against the risk of a further breach.

155. Plaintiff and the California Subclass also seek an order requiring Defendant to make full restitution of all monies it received through its wrongful conduct, along with all other relief permitted under Cal. Bus. & Prof. Code §§ 17200 *et seq.*

156. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 6
Confidentiality of Medical Information Act (CMIA) (Cal. Civ. Code § 56.06)
On behalf of Plaintiff and the California Subclass

157. Plaintiff, individually and on behalf of the Subclass, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

158. Defendant is a provider of healthcare under Cal. Civ. Code § 56.06, subdivisions (a) and (b), because it maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or make the information available to a health care provider, or for the diagnosis, treatment, or management of a medical condition.

159. Defendant is therefore subject to the requirements of the CMIA and obligated under Section 56.06 subdivision (e) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information that it maintains on behalf of users.

160. The CMIA defines medical information as meaning any "individually identifiable information" in possession of or derived from "a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." The information Defendant maintained and disclosed is medical information because "insurance policy/claim information" provides information about a subscriber's medical history, and was individually identifiable because it included information, including the subscriber's full name, full address, unique identifier, date of birth, and other information which "alone or in combination with other publicly available information reveals the identity of the individual."

161. Defendant violated Cal. Civ. Code Section 53.06(e) because it did not maintain the confidentiality of Plaintiff and Subclass members' medical information. This identifiable information was shared with third parties and it is unclear how far downstream the information

may have been shared including whether it may have been shared with criminal actors. In any event, no disclosure to Google Ads was ever authorized by the individual.

162. This negligent disclosure is in violation of Cal. Civ. Code Section 56.06(e) Accordingly, Plaintiff and Subclass members are entitled to: (1) nominal damages of $1,000 per violation pursuant to Cal. Civ. Code Section 53.36(b); (2) actual damages, in an amount to be determined at trial; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

163. Plaintiff also seeks such other relief as the Court may deem just and proper.

Court 7
Violation of California Penal Code § 631, *et. seq.* (Invasion of Privacy Act)
On behalf of Plaintiff and the Class

164. Plaintiff incorporates by reference and realleges each allegation in the paragraphs above as though fully set forth herein.

165. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature thereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630

166. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained**, or who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500)

167. Under CIPA, Blue Shield must show it had the consent of all parties to a communication.

168. At all relevant times, Blue Shield aided, employed, agreed with, and conspired with third parties, including Google, to track and intercept Plaintiff's and Class Members' internet communications. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiff and Class members.

169. Blue Shield intentionally inserted an electronic listening device, utilizing Google Analytics, onto Plaintiff's and Class Member's web browsers and devices that, without their knowledge or consent, tracked and transmitted the substance of their communication to Google and other unauthorized third parties, each of whom constitute a "Person" under the appropriate statute.

170. Blue Shield willfully facilitated the interception and collection of Plaintiff's and Class members' Private Information by intentionally using the Google Analytics tool and embedding it on their website.

171. Moreover, unlike past business tools such as the Facebook Like Button and older web beacons, Google Tag Manager, Google Analytics, and the other Tracking Tools are: (1) completely invisible to website and app users; and (2) Blue Shield has full control over these tools, including where they are embedded, what information is tracked and transmitted, and how events are categorized prior to their transmission.

172. Blue Shield's Tracking Technologies constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, they fall under the broad catch-all category of "any other manner."

173. Blue Shield failed to disclose its use of the Tracking Technologies to specifically track and automatically and simultaneously transmit Plaintiff's and Class Members' communications to Google and other undisclosed third-parties.

174. A portion of the Tracking Technologies—such as Google Analytics and GTM—are designed to transmit a website user's actions and communications contemporaneously as the user initiates each communication. As a result, the user's communications are intercepted in transit to the intended recipient—Blue Shield—before reaching Blue Shield's server.

175. Blue Shield violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time as they were made. Importantly, Google and other unauthorized third parties would not have intercepted or received the contents of these communications but for Blue Shield's actions, including its decision to install the Tracking Tools on its Web Properties.

176. By disclosing Plaintiff's and Class Members' Private Information, Blue Shield violated Plaintiff's and Class Members statutorily protected right to privacy.

177. As a result of these violations, and pursuant to CIPA section 637.2, Blue Shield is liable to Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for an amount of $5,000 per violation. Section 637.2 specifically states that: "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

178. Under the statute, Blue Shield is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

Court 8
Violation of California Penal Code § 638.51(a) (Invasion of Privacy Act)
On behalf of Plaintiff and the California Subclass

179. Plaintiff, individually and on behalf of the Subclass, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

180. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

181. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication." Cal. Penal Code § 638.50(b).

182. The Tracking Tools are "pen registers" because they are device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information" from Plaintiff and Class Members' electronic communications. *Id*.

183. At all relevant times, Blue Shield installed the Tracking Tools—which are pen registers—onto Plaintiff's and Class Members' browsers, and it used the Tracking Tools to collect Plaintiff's and Class Members' Private Information.

184. Plaintiff and Class Members did not provide their consent to Blue Shield's installation or use of the Tracking Tools.

185. Blue Shield did not obtain a court order to install or use the Tracking Tools.

186. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Blue Shield's violations of CIPA § 638.51(a), and each seek statutory damages of $5,000 for each of Blue Shield's violations of CIPA § 638.51(a)

Court 9
Invasion of Privacy Under California's Constitution (Article 1, §1)
On behalf of Plaintiff and the California Subclass

187. Plaintiff, individually and on behalf of the Subclass, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

188. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their Private Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites for the provision of insurance and healthcare without being subjected to wiretaps, pin registers, and/or trap and trace devices without their knowledge or consent.

189. By using Google Analytics and accompanying Tracking Technologies to communicate patients' individually identifying information alongside their confidential medical communications and insurance information, Blue Shield intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

190. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that Blue Shield would not install wiretaps, pin registers, and/or trap and trace devices to secretly transmit their communications and routing information.

191. Plaintiff and Class Members did not authorize Blue Shield to transmit their Private Information to third parties, nor did they consent to allowing third parties to intercept, receive, and view those communications.

192. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the right of privacy.

193. As a result of Blue Shield's actions, Plaintiff and Class members have suffered harm and injury, including but not limited to invasion of their privacy rights.

194. Plaintiff and Class Members have been damaged as a direct and proximate result of Blue Shield's invasion of privacy and are entitled to just compensation, including monetary damages.

195. Plaintiff and Class Members seek appropriate relief for this injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests.

196. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Blue Shield's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights.

197. Such damages are needed to deter Blue Shield from engaging from such conduct in the future. As described above, Blue Shield has a long history of exposing subscriber PII and PHI to unauthorized third-parties.

198. Plaintiff also seeks such other relief as the Court may deem just and proper.

Court 10
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq*.
On behalf of Plaintiff and the Nationwide Class

199. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

200. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

201. In relevant part, the ECPA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

202. The ECPA protects both sending and receipt of communications.

203. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

204. The transmissions of Plaintiff's Private Information via Blue Shield's Web Properties qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

205. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and Blue Shield via its Web Properties are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

206. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

207. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

208. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices and mobile devices.

c. Blue Shield's web-servers; and

d. The Tracking Tools deployed by Blue Shield to effectuate the sending and acquisition of subscriber communications.

209. When Plaintiff and Class Members interacted with Blue Shield's Web Properties, Blue Shield, through the Tracking Tools embedded and operating on its Web Properties, contemporaneously and intentionally disclosed, used, and redirected, and endeavored to disclose, use, and redirect, the contents of Plaintiff's and Class Members' electronic communications to third parties, including Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. §2511(1)(c)-(d).

210. Blue Shield's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff and Class Members regarding the PII and PHI.

211. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Facebook, Google, and Microsoft, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Blue Shield violated 18 U.S.C. § 2511(1)(c)-(d).

212. Blue Shield intentionally used the wire or electronic communications to increase its profit margins, and it specifically used the Tracking Tools to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

213. Blue Shield was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

214. Plaintiff and Class Members did not authorize Blue Shield to acquire the content(s) of their communications via the Tracking Tools for purposes of invading their privacy.

215. Any purported consent Blue Shield received from Plaintiff and Class Members was not valid.

216. Unauthorized Purpose. Blue Shield intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, breaches of confidence, invasion of privacy, among others.

217. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

218. Blue Shield is a "party to the communication" with respect to Plaintiff's and Class Members' communications, but its simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

219. More specifically, Blue Shield's acquisition of Plaintiff's and Class Members' communications, which were used and disclosed to unauthorized third parties, was done for the purpose of committing criminal and tortious acts in violation of the laws of the United States and California, including:

a. 42 U.S.C. § 1320d-6;

b. 45 CFR § 164.508(a)(1);

c. 15 U.S.C. § 45;

d. Cal. Penal Code § 631, et seq.;

e. Cal. Penal Code §638.51(a);

f. Cal. Civ. Code § 56, et seq.;

g. Cal. Bus. & Prof. Code § 17200; and

h. The common law causes of action alleged herein.

220. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

221. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

222. Blue Shield's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used persistent identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Google without patient authorization.

223. Blue Shield's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Blue Shield's use of the Tracking Technology was for its commercial advantage to increase revenue from existing patients and gain new patients.

224. Blue Shield is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications because Blue Shield used its participation in these communications to improperly share Private Information with third-parties that did not participate in these communications (e.g., Google) when Plaintiff and Class Members: (1) were unaware those third parties would receive their Private Information; and (2)did not consent to them receiving their Private Information.

225. Blue Shield accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

226. As such, Blue Shield cannot viably claim any exception to ECPA liability.

227. Plaintiff and Class Members have suffered damages as a direct and proximate result of Blue Shield's invasion of privacy.

228. As a result of Blue Shield's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

Court 11
Common Law Invasion of Privacy – Intrusion upon Seclusion
On behalf of Plaintiff and the Nationwide Class

229. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

230. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Blue Shield via its Web Properties.

231. Plaintiff and Class Members communicated sensitive and PHI and PII that they intended for only Blue Shield to receive and which they understood Blue Shield would keep private as their insurance provider and healthcare provider.

232. Blue Shield's disclosure of the substance and nature of Plaintiff's and Class Members' communications to third parties without their knowledge and consent is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

233. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential, and that Blue Shield would not install: (1) wiretaps to secretly transmit their communications to unauthorized third parties; or (2) pin registers and/or trap and trace devices.

234. Blue Shield was authorized to receive Plaintiff's and Class Members' Private Information, but it was not authorized to: (1) commandeer Plaintiff's and Class Members' web

browsers and devices, thereby forcing those devices to transmit information to Google without their consent or authorization.

235. As such, Blue Shield obtained Plaintiff's and Class Members' Private Information under false pretenses and/or exceeded its authority to obtain the Private Information.

236. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

237. Plaintiff and Class Members have been damaged as a direct and proximate result of Blue Shield's invasion of their privacy and are entitled to just compensation, including monetary damages.

238. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests.

239. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Blue Shield's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Blue Shield from engaging in such conduct in the future.

240. Plaintiff also seeks such other relief as the Court may deem just and proper.

Court 12
Common Law Invasion of Privacy – Publication of Private Facts
On behalf of Plaintiff and the Nationwide Class

241. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

242. Plaintiff's and Class Members' Private Information, including their communications and sensitive data, are private facts that third parties acquired without the knowledge or consent of Plaintiff and Class Members.

243. Defendant gave publicity to Plaintiff's and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties, including

Google, which builds massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

244. Plaintiff and Class Members did not know that Blue Shield was using software to track and disclose their Private Information.

245. Blue Shield's surreptitious tracking and commoditization of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person, particularly given that Blue Shield provides vision insurance, partners with healthcare providers to offer medical services, and is engaged in the business of owning and operating vision clinics.

246. In disseminating Plaintiff's and Class Members' personal information without their consent, Blue Shield acted with oppression, fraud, or malice.

247. Plaintiff and Class Members have been damaged by the publication of their Private Information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

Court 13
Common Law – Breach of Confidence
On behalf of Plaintiff and the Nationwide Class

248. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

249. Plaintiff and Class Members disclosed their Private Information in confidence with Blue Shield through Blue Shield's Web Properties.

250. Plaintiff and Class Members have an interest in keeping their PII and PHI confidential.

251. The information disclosed in confidence is PII and PHI and the Defendant knew was confidential due to Federal and State laws that protect such information (i.e., CIPA and HIPAA).

252. Plaintiff and Class Members had an expectation that the confidential information disclosed to Defendant would be kept in confidence with Defendant due to their relationship with

Defendant as a health services provider and Federal and State laws that protect such information (e.g., CIPA, CMIA, and HIPAA).

253. Blue Shield violated its duty to protect the confidentiality of Plaintiff's and Class Members' information by using Tracking Tools to communicate patients' Private Information with unauthorized third parties.

254. Blue Shield disclosed Plaintiff's and Class Members' confidential information for Blue Shield's own economic benefit in Blue Shield's own business and disclosing it without Plaintiff's and Class Members' consent.

255. Blue Shield disclosed and disseminated Plaintiff's and Class Members' confidential communications to a broad audience including Google and others.

256. At no time did Blue Shield offer to purchase or financially compensate Plaintiff and Class Members for the use of their confidential information for Blue Shield's advertising purposes.

257. As a result of Blue Shield's actions, Plaintiff and Class Members suffered harm and injury, including but not limited to a breach of their confidence, were damaged as a direct and proximate result of Blue Shield's breach, and are entitled to just compensation, including monetary damages.

258. Plaintiff also seeks such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and her counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: April 11, 2025

Respectfully submitted,

/s/ Amber L. Schubert

Robert C. Schubert (SBN 62684)
Amber L. Schubert (SBN 278696)
Daniel L.M. Pulgram (SBN 354569)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: 415-788-4220
Fax: 415-788-0161
rschubert@sjk.law
aschubert@sjk.law
dpulgram@sjk.law

Counsel for Plaintiff and the Proposed Classes